1. Entity posing the challenge

UPTEK: IBARMIA, LANTEK, LOIRE, ONA, ZAYER

2. Challenge

How can we secure the data generated by machines and their software? How can we improve cybersecurity in global asset management?

3. Possible solutions that can be applied

- Cybersecurity: securing assets/data and cyber-intelligence
- Software and hardware security engineering
- Security management and threat intelligence: monitoring and correlating threats
- Audits and risk mapping
- Technologies for strengthening remote access
- Digital identity and access management (IAM)

4. Context

Cybersecurity in the machine tools sector applies to both the products offered on the market, whether they are machines (Ibarmia, Loire, Ona and Zayer) or software (as in the case of Lantek), and the company's own production and work processes. This is because the machines and products offered have multiple interconnections to other machines and systems and the customer needs to be assured that connections are safe and secure at all times, while the company itself needs to be able to ensure that its own processes are also safe. In this context, the companies proposing the challenge have different problems and interests:

- Some of them have provided different web applications for years, which they connect to from the internet, and which they access from the cloud on multiple servers, and they need to ensure secure remote access. In this sense, as the solutions are deployed for several customers, it is important to manage the connections as a whole in order to monitor and respond to threats.
- Others have problems with secure access to remotely extract data from customers' machines.
- There is also the problem that some machinery sold may be sold again or used incorrectly by third parties. Therefore, it is proposed that the movement and location of machines needs to be controlled, and digital fingerprints need to be used to allow access to the machine.

In this context, help is needed from startups to define the security standards required for each company, and to apply solutions to achieve them, while ensuring that the proposals they make to the market as technology providers are secure for their customers, and positioning them at a higher competitive level than they are today.

5. Subsidiary challenges and objectives

In view of the above, and bearing in mind that the reality of the sector is that equipment is exposed to multiple vulnerabilities when connecting to other equipment, peripheral systems and software tools, companies must act to improve the security of the machine itself, and its connections, i.e. they must ensure that the machine is protected both externally and internally.

Consequently, the SMEs involved have posed 2 subsidiary challenges in relation to this challenge:

1. **To improve the securitisation of data**: as one of the main problems in cybersecurity today is data "exfiltration", i.e. data escape from the environment in which they are hosted. Many of the growing cyber-threats are no longer so much about data theft, but about falsifying data. For this reason, we propose tackling **the challenge of validating and managing the certification of the origin of data**.
2. Moreover, from a more holistic point of view, companies need solutions that allow them to **manage their assets in a comprehensive way so that they can monitor and respond to threats in a coordinated manner**. To this end, it would be interesting to have a start-up that could support the entire process to **ensure the overall security of assets and connections, firstly by carrying out digital forensic cybersecurity analyses** of their devices/protocols/connections to create a risk map and prioritise actions, and secondly to **set up a cybersecurity operations centre to prevent incidents, and monitor and respond to threats in real time**.

Last but not least, here are some of the questions that companies ask the market in order to contextualise some of the issues that we want to raise with the 2 subsidiary challenges above:

- Is it possible to monitor and trigger an automatic response to threats in a coordinated manner across the organisation?
- How can protection mechanisms be devised for the connection services offered to the customer in the product?
- Is it possible to develop warning and locking mechanisms to detect the movement of machines?
- How can secure connections to the organisation's network be ensured when staff connect externally?